

CLAIMS

1. - 37. (Canceled)

38. (Currently Amended) A method for controlling access to and tracking the routing of an electronic document, comprising:

embedding a control mark within an electronic document created by a document word processor, such that when

wherein the control mark remains embedded in the electronic document after changing a body of the electronic document is changed by with the document word processor after the control mark is embedded in the document, the control mark remains embedded in the document without having to re-embed the control mark in the document, and;

wherein the control mark cannot be changed by or removed by means of with the document word processor; and

wherein the control mark includes an encrypted check sum configured to self-authenticate or self-validate the electronic document; and
detecting at least one packet containing the electronic document transmitted over a network transmitted network packets containing the electronic document, based on the control mark, in order to block access to the electronic document from unauthorized recipients;
making a determination that the electronic document has been changed in response to detecting the control mark in the electronic document contained in the at least one packet; and
blocking access to the electronic document in response to the determination.

39. (Currently Amended) The method of claim 38 further comprising logging an audit record of the transmission, when a in response to detecting the at least one network packet containing the electronic document is detected by said detecting, wherein the audit record stores information identifying is configured to identify a distribution route of the electronic document.

40. (Currently Amended) The method of claim 39 wherein said logging the audit record includes logging a date and time of the transmission in the audit record.

41. (Currently Amended) The method of claim 39 wherein said logging the audit record includes logging a destination of the transmission in the audit record.

42. (Currently Amended) The method of claim 38 wherein said detecting monitors network packets at least one packet includes detecting at least one packet transmitted internally within an organization the network.

43. (Currently Amended) The method of claim 38 wherein said detecting monitors network packets at least one packet includes detecting at least one packet transmitted from within an organization the network to outside of the organization an external network.

44. (Currently Amended) The method of claim 38 wherein said detecting monitors network packets at least one packet includes detecting at least one packet transmitted to an organization the network from outside of the organization an external network.

45. (Currently Amended) The method of claim 38 wherein the network packets are at least one packet is transmitted in response to an FTP download.

46. (Currently Amended) The method of claim 38 wherein the network packets are at least one packet is transmitted in response to an HTTP download.

47. (Currently Amended) The method of claim 38 wherein the network packets are at least one packet is transmitted in response to an Instant Messenger download.

Previously Submitted
COPY

48. (Currently Amended) A ~~system for controlling access to and tracking the routing of an electronic document, the system comprising one or more tangible computer readable media collectively storing instructions encoding~~ memory device having instructions stored thereon that, in response to execution by a processing device, cause the processing device to perform operations comprising:

~~an auto-marking module for embedding a control mark within an electronic document created by a document word processor, such that when~~

wherein the control mark remains embedded in the electronic document after changing a body of the electronic document is changed by with the document word processor after the control mark is embedded in the document, the control mark remains embedded in the document without having to re-embed the control mark in the document; and

wherein the control mark cannot be changed by or removed with by means of the document word processor; and

wherein the control mark includes an encrypted check sum configured to self-authenticate or self-validate the electronic document; and

~~a traffic monitor for detecting transmitted network packets containing the electronic document, based on the control mark, in order to block access to the electronic document from unauthorized recipients;~~

making a determination that the electronic document contained in at least one of the transmitted packets has been changed; and

blocking access to the electronic document contained in the at least one of the transmitted packets in response to the determination.

49. (Currently Amended) The ~~system~~ memory device of claim 48 wherein ~~the one or more media further store instructions encoding an auditor for execution of the instructions cause the processing device to perform operations further comprising~~ logging transmission information including a distribution route of the electronic document in an audit record ~~when a network packet containing the electronic document is detected by said traffic monitor, wherein the audit record stores information identifying a distribution route of the electronic document in response to detecting the transmitted network packets.~~

50. (Currently Amended) The system memory device of claim 49 wherein said auditor logs a date and time of the network packet's transmission in the audit record includes a date and time associated with detecting the transmitted network packets.

51. (Currently Amended) The system memory device of claim 49 wherein said auditor logs a destination for the network packet in the audit record includes a destination of the transmitted network packets.

52. (Currently Amended) The system memory device of claim 48 wherein said traffic monitor monitors detecting further includes monitoring network packets transmitted internally within an organization network.

53. (Currently Amended) The system memory device of claim 48 wherein said traffic monitor monitors detecting further includes monitoring network packets transmitted from within an internal organization network to outside of the an external organization network.

54. (Currently Amended) The system memory device of claim 48 wherein said traffic monitor monitors detecting further includes monitoring network packets transmitted to an internal organization network from outside of the an external organization network.

55. (Currently Amended) The system memory device of claim 48 wherein the said detecting transmitted network packets are transmitted occurs in response to an FTP download.

56. (Currently Amended) The system memory device of claim 48 wherein the said detecting transmitted network packets are transmitted occurs in response to an HTTP download.

Previously Submitted
COPY

57. (Currently Amended) The system memory device of claim 48 wherein the said detecting transmitted network packets are transmitted occurs in response to an Instant Messenger download.

58. - 90. (Canceled)

Previously Submitted
COPY